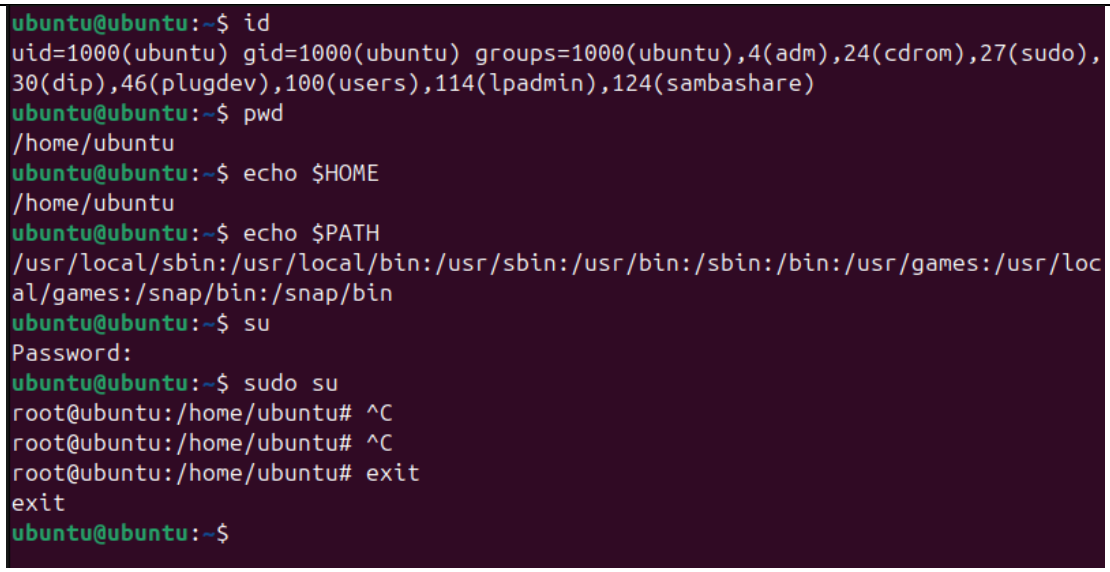
Practical 2

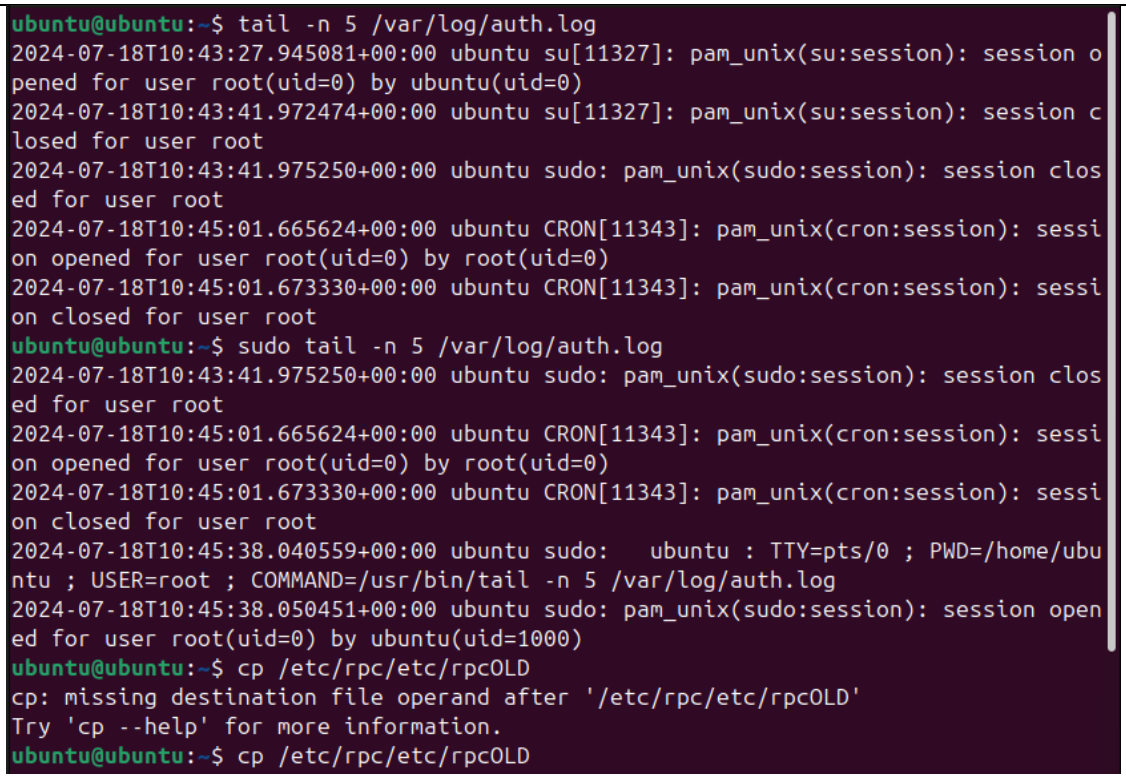
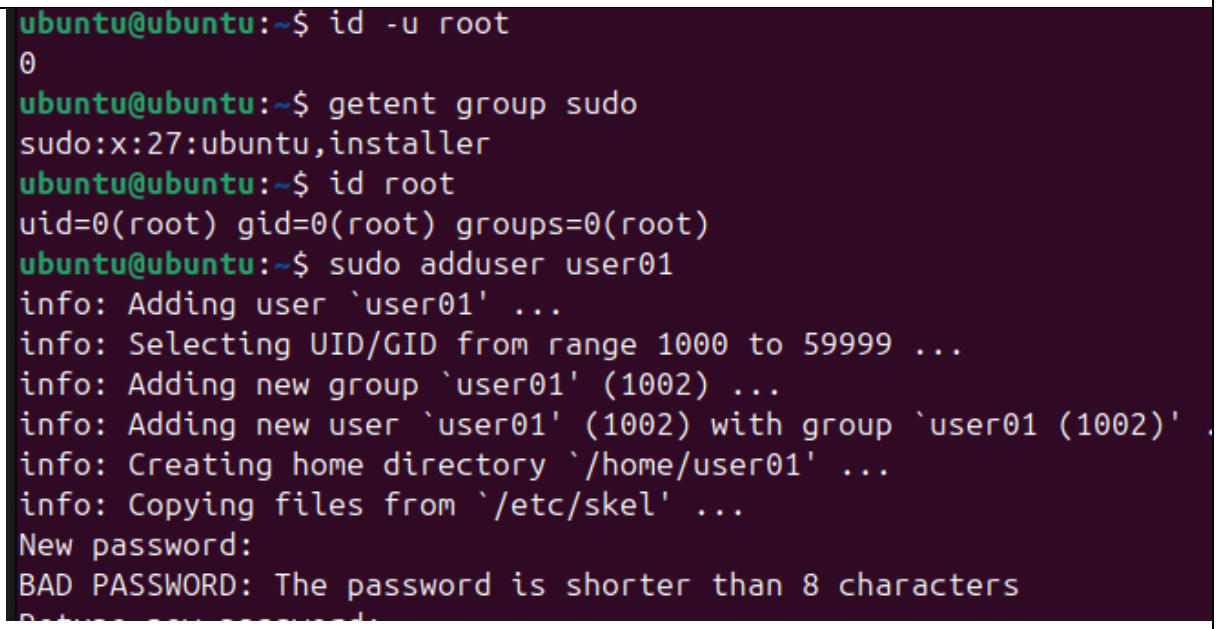
Aim: User Administration
1. Manage local users, groups and creation of multiple users from excel sheet
2. Control access to files
Commands for reference:
System Administrator: su, adduser, addgroup, rmuser, shutdown
Control Access: chmod, umask

PART A

Manage local users, groups and creation of multiple users from excel sheet

Que.	1. Run id command to view the current user and group information. 2. display the current working directory. 3. print the value of HOME and PATH variable to determine the home directory and user's executable's path respectively. 4. Run su and su - command. Observe the output for the same.what is the main difference between them? 5. Run sudo su at the shell prompt to become the root user. 9. Exit the current user's shell to return to the student user's shell
Command	1. id 2. pwd 3. echo $HOME 4. echo $PATH 5. su 6. su - • su: Switches to the target user's shell but retains the current environment. • su -: Switches to the target user's shell and initiates a new login shell, effectively switching to the target user's environment. 7. sudo su 8. exit

Output	
Que	10. Attempt to view the last five lines of /var/log/auth.log without using sudo 11. Attempt to view the last five lines of /var/log/auth.log using sudo 12. Attempt to make a copy of /etc/rpc as /etc/rpcOLD without using sudo 13. Attempt to make a copy of /etc/rpc as /etc/rpcOLD with sudo. 14. Attempt to delete /etc/rpcOLD without using sudo 15. Attempt to delete /etc/rpcdOLD with sudo
Commands	10.tail -n 5 /var/log/auth.log 11.sudo tail -n 5 /var/log/auth.log 12.cp /etc/rpc /etc/rpcOLD 13.sudo cp /etc/rpc /etc/rpcOLD 14.rm /etc/rpcOLD 15.sudo rm /etc/rpcOLD

Output	
Que	16. check the UID for root user, administrator and local users. 17. Adduser user01.
Commands	10. id -u root getent group sudo id root 11. sudo adduser user01
Output	

```
tematic
Retype new password:
passwd: password updated successfully
Changing the user information for user01
Enter the new value, or press ENTER for the default
        Full Name []: user01
        Room Number []: 1
        Work Phone []: 9988776655
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `user01' to supplemental / extra groups `user
info: Adding user `user01' to group `users' ...
ubuntu@ubuntu:~$
```

Que.	18. Create the group group01 with the GID of 10000. 19. Create the group group02 20. Examine /etc/group to verify the supplemental group memberships.
Command	18. sudo addgroup --gid 10000 group01sudo 19. sudo addgroup group02 20. cat /etc/group
Output	

```
ubuntu@ubuntu:~$ sudo groupadd -g 1001 grp2
groupadd: GID '1001' already exists
ubuntu@ubuntu:~$ sudo groupadd -g 2001 grp2
ubuntu@ubuntu:~$ sudo group add grp3
sudo: group: command not found
ubuntu@ubuntu:~$ sudo groupadd grp3
ubuntu@ubuntu:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu,installer
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:installer
fax:x:21:
voice:x:22:
```

Que.	
Command	
Output	

```
fwupd-refresh:x:989:
scanner:x:115:saned
saned:x:116:
geoclue:x:117:
pipewire:x:118:
polkitd:x:988:
rtkit:x:119:
colord:x:120:
gdm:x:121:
nm-openvpn:x:122:
lxd:x:123:installer
ubuntu:x:1000:
sambashare:x:124:ubuntu
gamemode:x:987:
gnome-initial-setup:x:986:
gnome-remote-desktop:x:985:
installer:x:1001:
user01:x:1002:
group01sudo:x:10000:
group02:x:10001:
grp1:x:10002:
grp2:x:2001:
grp3:x:10003:
ubuntu@ubuntu:~$
```

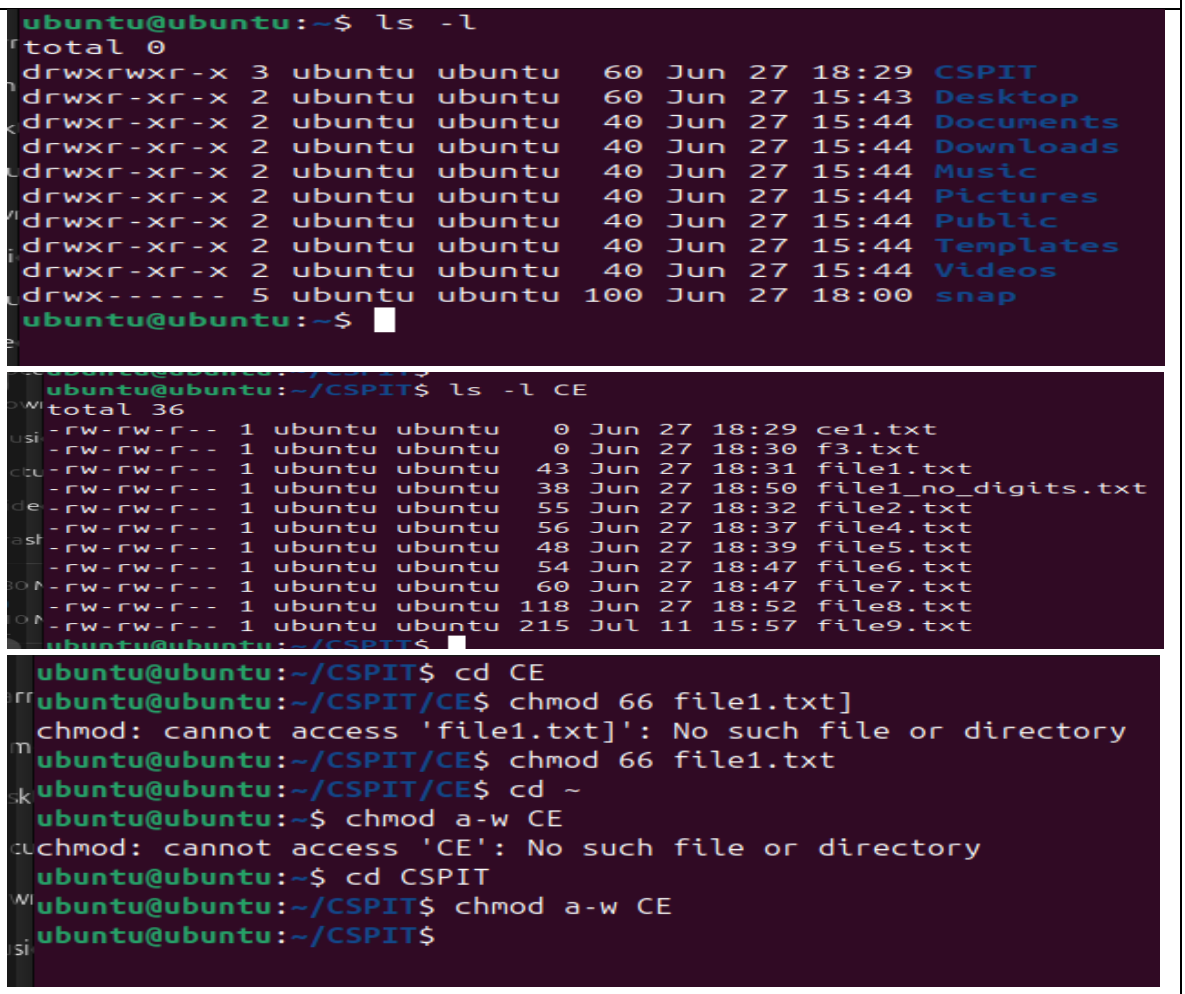
Que.	21. Use the usermod -aG command to add a user to a supplementary group. Add user01 to the group created. 22. Observe /etc/group and /etc/passwd
Command	21. sudo usermod -aG group01 user01 22. cat /etc/group

Output

```
ubuntu@ubuntu:~$ sudo usermod -aG grp31 user01
usermod: group 'grp31' does not exist
ubuntu@ubuntu:~$ sudo usermod -aG grp3 user01
ubuntu@ubuntu:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu,installer
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:installer
fax:x:21:
voice:x:22:
```

```
fwupd-refresh:x:989:
scanner:x:115:saned
saned:x:116:
geoclue:x:117:
pipewire:x:118:
polkitd:x:988:
rtkit:x:119:
colord:x:120:
gdm:x:121:
nm-openvpn:x:122:
lxd:x:123:installer
ubuntu:x:1000:
sambashare:x:124:ubuntu
gamemode:x:987:
gnome-initial-setup:x:986:
gnome-remote-desktop:x:985:
installer:x:1001:
user01:x:1002:
group01sudo:x:10000:
group02:x:10001:
grp1:x:10002:
grp2:x:2001:
grp3:x:10003:user01
ubuntu@ubuntu:~$
```

PART B
Control access to files

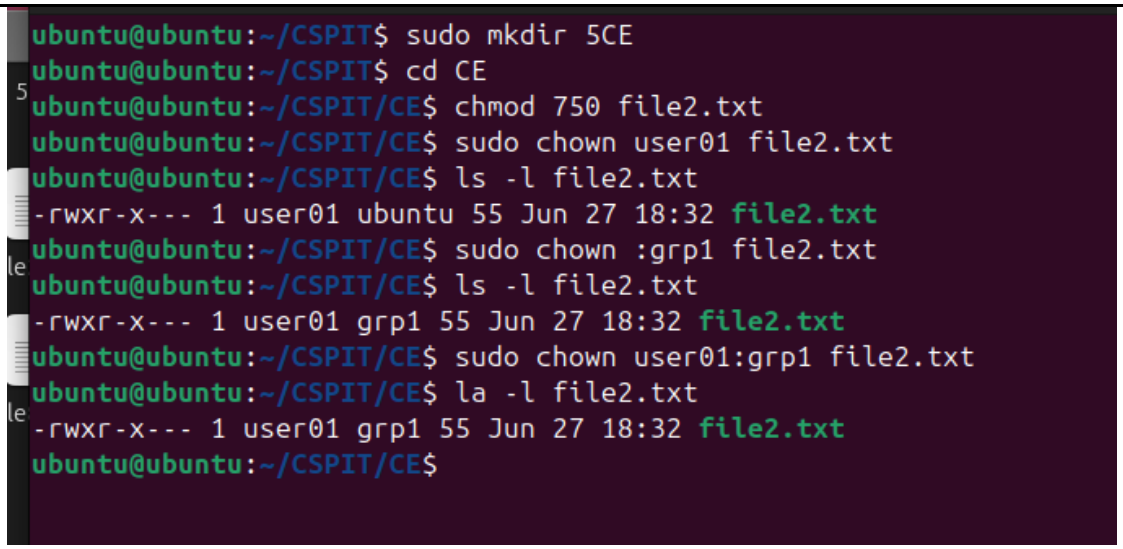
Que.	1. Check the permission of files created. 2. Check the permission of directories created. 3. Set read and write permissions for others with numeric mode to file1.txt 4. Remove write permission for user, group and others to folder CE.
Command	1. ls -l file2.txt 2. ls -ld CE 3. chmod 666 file1.txt 4. chmod a-w CE
Output	

```
ubuntu@ubuntu:~$ ls -l
total 0
drwxrwxr-x 3 ubuntu ubuntu  60 Jun 27 18:29 CSPIT
drwxr-xr-x 2 ubuntu ubuntu  60 Jun 27 15:43 Desktop
drwxr-xr-x 2 ubuntu ubuntu  40 Jun 27 15:44 Documents
drwxr-xr-x 2 ubuntu ubuntu  40 Jun 27 15:44 Downloads
drwxr-xr-x 2 ubuntu ubuntu  40 Jun 27 15:44 Music
drwxr-xr-x 2 ubuntu ubuntu  40 Jun 27 15:44 Pictures
drwxr-xr-x 2 ubuntu ubuntu  40 Jun 27 15:44 Public
drwxr-xr-x 2 ubuntu ubuntu  40 Jun 27 15:44 Templates
drwxr-xr-x 2 ubuntu ubuntu  40 Jun 27 15:44 Videos
drwx------ 5 ubuntu ubuntu 100 Jun 27 18:00 snap
ubuntu@ubuntu:~$
```

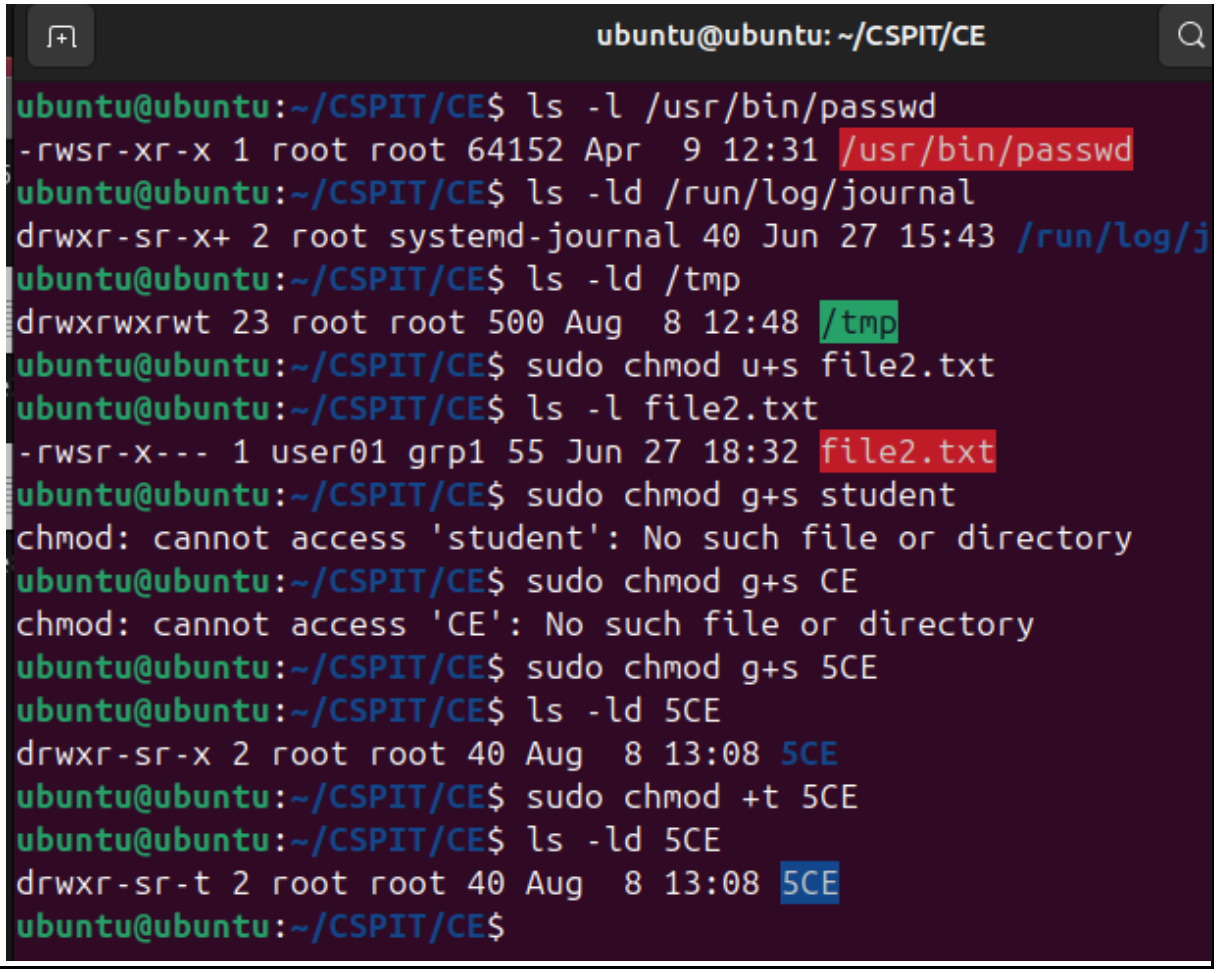
```
ubuntu@ubuntu:~/CSPIT$ ls -l CE
total 36
-rw-rw-r-- 1 ubuntu ubuntu   0 Jun 27 18:29 ce1.txt
-rw-rw-r-- 1 ubuntu ubuntu   0 Jun 27 18:30 f3.txt
-rw-rw-r-- 1 ubuntu ubuntu  43 Jun 27 18:31 file1.txt
-rw-rw-r-- 1 ubuntu ubuntu  38 Jun 27 18:50 file1_no_digits.txt
-rw-rw-r-- 1 ubuntu ubuntu  55 Jun 27 18:32 file2.txt
-rw-rw-r-- 1 ubuntu ubuntu  56 Jun 27 18:37 file4.txt
-rw-rw-r-- 1 ubuntu ubuntu  48 Jun 27 18:39 file5.txt
-rw-rw-r-- 1 ubuntu ubuntu  54 Jun 27 18:47 file6.txt
-rw-rw-r-- 1 ubuntu ubuntu  60 Jun 27 18:47 file7.txt
-rw-rw-r-- 1 ubuntu ubuntu 118 Jun 27 18:52 file8.txt
-rw-rw-r-- 1 ubuntu ubuntu 215 Jul 11 15:57 file9.txt
```

```
ubuntu@ubuntu:~/CSPIT$ cd CE
ubuntu@ubuntu:~/CSPIT/CE$ chmod 66 file1.txt]
chmod: cannot access 'file1.txt]': No such file or directory
ubuntu@ubuntu:~/CSPIT/CE$ chmod 66 file1.txt
ubuntu@ubuntu:~/CSPIT/CE$ cd ~
ubuntu@ubuntu:~$ chmod a-w CE
chmod: cannot access 'CE': No such file or directory
ubuntu@ubuntu:~$ cd CSPIT
ubuntu@ubuntu:~/CSPIT$ chmod a-w CE
ubuntu@ubuntu:~/CSPIT$
```

Que.	5. Create a directory 5CE under CE. Observe the response. 6. Set read, write and execute permissions for user, group and others to 5CE. 7. Set read and execute permission for group and no permission for other to file2.txt. 8. Change the ownership of file to user01 9. Change the group ownership of file to group01 10. Change the ownership of both group and user at the same time.

Command	5. mkdir CE/5CE 6. chmod 777 CE/5CE 7. chmod 750 file2.txt 8. sudo chown user01 file2.txt 9. sudo chown :group01 file2.txt 10. sudo chown user01:group01 file_name
Output	

Que.	11. Set the special permissions on directory. a. The *setuid* permission on an executable file means that commands run as the user owning the file, not as the user that ran the command. One example is the passwd command:run ls -l /usr/bin/passwd b. The special permission *setgid* on a directory means that files created in the directory inherit their group ownership from the directory, rather than inheriting it from the creating user. run ls -ld /run/log/journal c. the *sticky bit* for a directory sets a special restriction on deletion of files. Only the owner of the file (and root) can delete files within the directory. run ls -ld /tmp 12. Set the setusid, setgid and sticky bit for different files and perform the operations accordingly.
Command	11. a) ls -l /usr/bin/passwd b) ls -ld /run/log/journal c) ls -ld /tmp 12. sudo chmod u+s file_name sudo chmod g+s directory_name sudo chmod +t directory_name

Output	

Que.	13. Display the current value of shell's mask. 14. Check the permission of directories. 15. Check the permission of files. 16. Set the umask to 542. 17. Check the permission of files and directories. 18. Try to open the file and directory created. 19. Try to open the file as other user.
Command	13. umask 14. ls -ld directory_name 15. ls -l file_name 16. umask 542 17. touch new_file mkdir new_directory ls -l new_file ls -ld new_directory 18. cat new_file cd new_directory 19. su another_user cat new_file

Output

```
ubuntu@ubuntu:~/CSPIT/CE$ sudo mkdir newdir
ubuntu@ubuntu:~/CSPIT/CE$ ls -l ce1.txt
-rw-rw-r-- 1 ubuntu ubuntu 0 Aug  8 13:20 ce1.txt
ubuntu@ubuntu:~/CSPIT/CE$ ls -ld mkdir
ls: cannot access 'mkdir': No such file or directory
ubuntu@ubuntu:~/CSPIT/CE$ ls -ld newdir

drwxr-xr-x 2 root root 40 Aug  8 13:20 newdir
ubuntu@ubuntu:~/CSPIT/CE$ cat ce1.txt
ubuntu@ubuntu:~/CSPIT/CE$ cd newdir
ubuntu@ubuntu:~/CSPIT/CE/newdir$ su another_user
su: user another_user does not exist or the user entry does not co
the required fields
ubuntu@ubuntu:~/CSPIT/CE/newdir$ adduser another_user
fatal: Only root may add a user or group to the system.
ubuntu@ubuntu:~/CSPIT/CE/newdir$ su user01
Password:
user01@ubuntu:/home/ubuntu/CSPIT/CE/newdir$ cat ce1.txt
```

```
ubuntu@ubuntu:~/CSPIT/CE$ cd newdir
ubuntu@ubuntu:~/CSPIT/CE/newdir$ su user01
Password:
user01@ubuntu:/home/ubuntu/CSPIT/CE/newdir$ cat ce1.txt
user01@ubuntu:/home/ubuntu/CSPIT/CE/newdir$ cat ce1.txt
hello students . hello students
user01@ubuntu:/home/ubuntu/CSPIT/CE/newdir$
```